PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-030028
(43)Date of publication of application : 28.01.2000

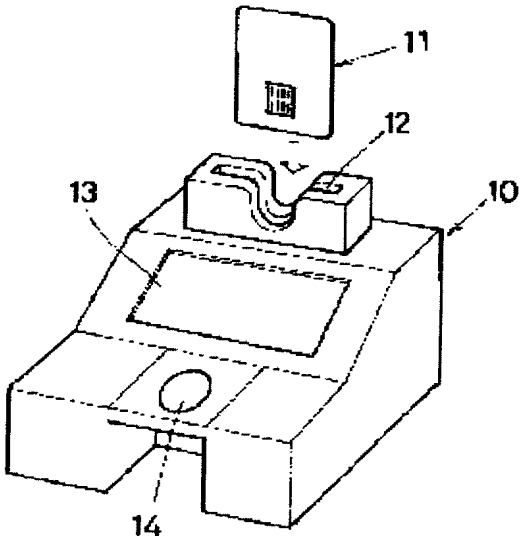
(51)Int.Cl. G06K 19/10
G06K 17/00
G07F 7/12
// G07G 1/14

(21)Application number : 10-193013
(22)Date of filing : 08.07.1998

(71)Applicant : OMRON CORP
(72)Inventor : TATEISHI SHUNZO
MORITA SHOSUKE

(54) AUTHENTICATION MEDIUM, AUTHENTICATION MEDIUM ISSUING DEVICE, AND AUTHENTICATING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the security of application by constituting an authentication medium so that biometric information can be recorded on and read out of a recording medium such as an IC card and a SIM chip.
SOLUTION: Necessary items of respective files are inputted by a keyboard and then user's authentication card such as an IC card and a SIM is inserted into an insertion slot 12. Then, the read of biometric information of the user is guided and displayed on a display unit 13, and when the user places a specific finger on a sensor 14 to read the fingerprint out, fingerprint information is taken in and the feature quantity of the fingerprint is read according to the matching level and matching score of set attribute data. Thus, when the user's fingerprint information is determined together with its attribute data, they are written to the authentication card 11 together with the necessary items which are already inputted to constitute the authentication medium.



R1

全項目

(19)【発行国】日本国特許庁(JP)
(12)【公報種別】公開特許公報(A)
(11)【公開番号】特開2000－30028(P2000－30028A)
(43)【公開日】平成12年1月28日(2000．1．28)
(54)【発明の名称】認証媒体、認証媒体発行装置、及び認証装置
(51)【国際特許分類第7版】

G06K 19/10
17/00

G07F 7/12
// G07G 1/14

【FI】

G06K 19/00 S
17/00 B
V
G07G 1/14
G07F 7/08 B

【審査請求】未請求
【請求項の数】8
【出願形態】OL
【全頁数】9
(21)【出願番号】特願平10－193013
(22)【出願日】平成10年7月8日(1998．7．8)
(71)【出願人】
【識別番号】000002945
【氏名又は名称】オムロン株式会社
【住所又は居所】京都府京都市右京区花園土堂町10番地
(72)【発明者】
【氏名】立石 俊三
【住所又は居所】京都府京都市右京区花園土堂町10番地 オムロン株式会社内
(72)【発明者】
【氏名】森田 章介
【住所又は居所】京都府京都市右京区花園土堂町10番地 オムロン株式会社内
(74)【代理人】
【識別番号】100067747
【弁理士】
【氏名又は名称】永田 良昭
【テーマコード(参考)】

3E042
3E044
5B035
5B058

【Fターム(参考)】

3E042 BA17 BA18 CC02
3E044 AA09 AA20 BA04 CA06 CA07 CA10 DA05 DC05
5B035 AA06 AA13 AA14 BB09 BC01 CA11 CA22 CA29 CA38
5B058 CA13 CA25 KA02 KA04 KA11 KA32 KA38 YA02

(57)【要約】
【課題】この発明は、利用者のバイオメトリック情報を利用者が所有するICカードやシムチップ（SIMチップ）などの記録媒体に記録して利用者に所持させることにより、アプリケーション側の記憶容量を少なくして信頼性の高い本人の認証ができる認証媒体の提供を目的とする。
【解決手段】この発明は、個人情報と共に、指紋、声紋、網膜紋、顔面特徴、掌の紋など、個人を特定できる特徴部分で構成したバイオメトリック情報を読出し可能な記録媒体に記憶した認証媒体、該認証媒体を発行する認証媒体発行装置、および認証処理を行う認証装置であることを特徴とする。

【特許請求の範囲】
【請求項1】バイオメトリック情報を読出し可能な記録媒体に記憶した認証媒体。
【請求項2】上記バイオメトリック情報の照合レベル、照合スコア等の属性情報を記録した請求項1記載の認証媒体。
【請求項3】複数のセキュリティレベルに対応した属性情報を記録した請求項1記載の認証媒体。
【請求項4】認証が得られたときアプリケーションの可動を許容する情報を記録した請求項1記載の認証媒体。
【請求項5】認証が得られないとき記録情報の読出しを不可能にする破壊手段を備えた請求項1記載の認証媒体。
【請求項6】請求項1乃至5記載の内の1つの認証媒体を発行する装置であって、認証媒体に情報を記録する記録手段と、バイオメトリック情報を読取る読取り手段と、前記読取り手段で読取ったバイオメトリック情報を記録手段で認証媒体に記録制御する制御手段とを備えた認証媒体発行装置。
【請求項7】バイオメトリック情報の属性情報を入力する入力手段と、前記入力手段で入力した属性情報を記録手段で記録制御する制御手段とを備えた請求項6記載の認証媒体発行装置。
【請求項8】請求項1乃至5記載の内の1つの認証媒体を受入れて利用者を認証する装置であって、前記認証媒体から情報を読取る第1の読取り手段と、利用者のバイオメトリック情報を読取る第2の読取り手段と、第1の読取り手段が読取った認証媒体に記録のバイオメトリック情報と、第2読取り手段が読取った利用者のバイオメトリック情報とを比較して利用者本人を判定する判定手段とを備えた認証装置。

【発明の詳細な説明】
【0001】
【発明が属する技術分野】この発明は、例えば、金融・流通等の決済において本人を認証することができるような認証媒体、認証媒体発行装置、及び認証装置に関する。
【0002】
【従来の技術】従来、上述例の金融・流通等の決済分野においては高いセキュリティが要求されるので、処理を実行する本人の認証も信頼性の高い認証が要求される。例えば、上述の決済処理を実行するアプリケーション側に、利用者の指紋を読取るバイオメトリックセンサ（指紋読取り装置、CCDアレイで構成）と、予め登録した利用者の指紋情報を記憶した記憶手段とを備え、利用者が決済処理を行うとき、利用者の指紋をバイオメトリックセンサで読取り、記憶手段に記憶されている指紋情報と比較して同じと判定されることで本人の認証が得られるように構成することができる。
【0003】このように構成した場合、アプリケーション側には、操作の対象となる利用者全員のバイオメトリック情報（例えば、指紋情報）を記憶手段に記憶する必要があり、記憶容量が極めて多くなる問題点を有する。
【0004】
【発明が解決しようとする課題】この発明は、利用者のバイオメトリック情報を利用者が所有するICカードやシムチップ（SIMチップ）などの記録媒体に記録して利用者に所有させることにより、アプ

ン側の記憶容量を少なくして信頼性の高い本人の認証ができる認証媒体の提供を目的

]さらに、各アプリケーション側に設けられるバイオメトリックセンサの読取り性能にばらつ
っても、良好な本人認証ができ、さらに、それぞれのアプリケーションに設定されたセキュリ
ンベルに対応させて本人認証ができ、さらに、本人認証が得られたときアプリケーションの可
を許容することにより、アプリケーションのセキュリティを高めることができ、さらにまた、認証媒
体の悪用を防止することのできる認証媒体の提供を目的とする。さらに、上述の目的を達成する
認証媒体を発行することのできる認証媒体発行装置の提供を目的とする。さらにまた、前述の目
的を達成する認証媒体による本人認証が可能な認証装置の提供を目的とする。

【0006】

【課題を解決するための手段】この発明の請求項1記載の発明は、バイオメトリック情報を読出し可能な記録媒体に記憶した認証媒体であることを特徴とする。

【0007】この発明の請求項2記載の発明は、上記請求項1記載の発明の構成に併せて、上記バイオメトリック情報の照合レベル、照合スコア等の属性情報を記録した認証媒体であることを特徴とする。

【0008】この発明の請求項3記載の発明は、上記請求項1記載の発明の構成に併せて、複数のセキュリティレベルに対応した属性情報を記録した認証媒体であることを特徴とする。

【0009】この発明の請求項4記載の発明は、上記請求項1記載の発明の構成に併せて、認証が得られたときアプリケーションの可動を許容する情報を記録した認証媒体であることを特徴とする。

【0010】この発明の請求項5記載の発明は、上記請求項1記載の発明の構成に併せて、認証が得られないとき記録情報の読出しを不可能にする破壊手段を備えた認証媒体であることを特徴とする。

【0011】この発明の請求項6記載の発明は、請求項1乃至5記載の内の1つの認証媒体を発行する装置であって、認証媒体に情報を記録する記録手段と、バイオメトリック情報を読取る読取り手段と、前記読取り手段で読取ったバイオメトリック情報を記録手段で認証媒体に記録制御する制御手段とを備えた認証媒体発行装置であることを特徴とする。

【0012】この発明の請求項7記載の発明は、上記請求項6記載の発明の構成に併せて、バイオメトリック情報の属性情報を入力する入力手段と、前記入力手段で入力した属性情報を記録手段で記録制御する制御手段とを備えた認証媒体発行装置であることを特徴とする。

【0013】この発明の請求項8記載の発明は、請求項1乃至5記載の内の1つの認証媒体を受入れて利用者を認証する装置であって、前記認証媒体から情報を読取る第1の読取り手段と、利用者のバイオメトリック情報を読取る第2の読取り手段と、第1の読取り手段が読取った認証媒体に記録のバイオメトリック情報と、第2読取り手段が読取った利用者のバイオメトリック情報とを比較して利用者本人を判定する判定手段とを備えた認証装置であることを特徴とする。

【0014】

【発明の作用・効果】この発明の認証媒体によれば、指紋、声紋、網膜紋、顔面特徴等で代表されるバイオメトリック情報を、読み出し可能なICカードやSIMチップ等で代表される記録媒体に記録して読み出し可能なように認証媒体を構成したので、アプリケーション側には、操作の対象となる利用者全員のバイオメトリック情報を記憶手段に記憶して保存する必要がなく、アプリケーション側の記憶容量が極めて少なくて済む。また、1つの認証媒体を、例えば、銀行、クレジット社、郵便局、その他の金融機関、その他認証が必要な機関といつた業種の異なる複数のアプリケーションに対して使用することができ、便利性を有する。

【0015】また、バイオメトリック情報の属性情報として、例えば、バイオメトリック情報を読取る読取り手段の閾値レベルを設定した照合レベルや、バイオメトリック情報を照合して判定するときの基準値となる特徴点のポイント数を設定した照合スコアを記録すると、バイオメトリック情報を照合するための読取り手段に読取り精度のバラツキがあっても、また、利用者側に読取り時の状態に多少変動があっても、照合精度を調整することにより、照合に必要な情報の読取りができ、また、認証装置が複数あっても、同じ条件で照合ができ、利用者が本人であっても機械側の問題で、認証不可となることが防止される。

【0016】さらに、バイオメトリック情報の属性情報として、セキュリティレベルに対応した情報を記録しておくことにより、アプリケーション側のセキュリティレベルに対応した照合ができ、便利性を有する。

【0017】さらに、認証処理を実行しても認証が得られない場合、第3者の不正利用と判定される

ので、この場合、記録情報を破壊手段で読取り不可能にすることで、認証媒体のセキュリティを高めることができ、偽造防止対策にもなる。
【0018】さらに、認証媒体発行装置にあっては上述のような効果を奏する認証媒体の発行ができ、また、認証装置は、上述のような効果を奏する認証媒体の認証処理ができ、また、これらの認証媒体発行装置及び認証装置はいずれか1方で相互の機能を兼ねることができる。
【0019】
【実施例】この発明の一実施例を以下図面と共に説明する。図面は認証カードと認証装置を示し、図1において、認証装置10は認証カード11を挿入する挿入口12と、操作案内やその他の情報を表示すると共に、必要事項の入力を行うタッチパネル付きの表示器13と、操作者の指紋を読取るためのCCDアレイで構成されるバイオメトリックセンサ14を備え、さらに、該認証装置10は上位の機器、例えば、パーソナルコンピュータ(図示省略)に接続されて、各種のアプリケーションを駆動する。
【0020】前述の認証カード11はICカードで形成しており、該ICカードには所持者の個人情報とバイオメトリック情報として所持者の指紋情報及びその他の必要な情報を記録している。
【0021】このような認証カード11は認証装置10の挿入口12に挿入されると、内部のICカードリーダによりカード情報が読取られ、次いで認証カード所持者の登録した指をバイオメトリックセンサ14の上面に載置して指紋を読取り、この読取った指紋情報と、認証カード11に記録された指紋情報とを比較して、指紋の一致が判定されると本人が認証される。なお、本人認証が得られると、この認証装置10を接続しているパーソナルコンピュータの所定のアプリケーションの操作が許容される。あるいは、この認証装置10に接続された端末が能動化される。
【0022】図2は、上述の認証装置10の制御回路ブロック図を示し、CPU20はROM21に格納されたプログラムに沿って各回路装置を駆動制御し、フラッシュRAMで構成したRAM22は動作に必要なデータを記憶する。タッチパネル23は表示器13の表示に対応してタッチ入力し、ICカードリーダ24は前述の挿入口12の内部に設けられて挿入されたICカードで構成された認証カード11に対してカードデータの読取り/書込みを行う。接点出力端子25はこれに接続された機器、例えば、自動取引き処理装置に本人認証の結果を出力する。上位インターフェース回路26は上位であるパーソナルコンピュータ(PC)と接続してデータの送受信を行う。また、上述のパーソナルコンピュータ(PC)は、この認証装置10が認証カード11の発行装置として使用したとき、認証カード11に個人情報等必要なカードデータの入力手段となる。
【0023】図3は、前述の認証カード11の制御回路ブロック図を示し、CPU30はROM31に格納されたプログラム及び設定データに基づいて各回路装置を駆動制御し、フラッシュRAMで構成したRAM32は動作に必要なデータを記憶する他、カードデータを記憶する。なお、これらのCPU30、ROM31、RAM32は1チップで構成される。ICコンタクト33は認証装置10のICカードリーダ15と接続される。
【0024】ヒューズROM34は電気的に電気回路を破壊(溶断)する機能を有し、このROM34には電源投入時にプログラムをスタートさせるベクターアドレスが記録されており、したがって、このヒューズROM34の回路が破壊されるとプログラムがスタートできなくなり、その結果、カードデータが不正に読出されることなく保護でき、認証カードのセキュリティが高められる。
【0025】また、ヒューズROM書込み制御回路35は、上述のヒューズROM34にサイト電源を供給して該ROM34を破壊するための回路であって、CPU30により制御される。
【0026】図4は、前述の認証カード11のフラッシュRAM32に記録されるカードデータを示し、該カードデータは、マスターファイル、認証ファイル、パーソナルファイルの3つのファイルで構成している。
【0027】上述のマスターファイルは、発行者鍵であって発行者を示すコード番号のような情報であり、この発行者鍵が照合時に適性と判定されない時は認証ファイルの読取り/書込みが許容されない。
【0028】前述のマスターファイルは、管理者情報、管理者PIN(暗証番号)、管理者端末鍵の3つの小ファイルからなり、管理情報は、認証ユニット番号(認証装置番号)、管理端末番号、照合レベル、照合スコア、位置情報、読取りミス回数で構成している。
【0029】上述の認証ユニット番号は認証装置10の機番を示し、該認証装置10の制御部のROMに記録されている機番を記録している。管理端末番号は操作可能な端末の機番を示し、上位コンピュータのプログラムに記録されている機番を記録している。照合レベルは、バイオメトリックセンサ14が指紋を読取る時の閾値レベルの設定値を示し、該照合レベルは認証装置10毎に設定することができる。照合スコアは指紋の特徴点のポイント数を示す。位置情報は特徴点の中心部の

X. Yの座標値を示し、バイオメトリックセンサ14が指紋を読取って照合する時指紋情報の位置合せに利用される。読取りミス回数は認証NG結果を計数した計数値であり、所定回数以上のNGがあれば認証カード11を電気的に破壊して使用不可にする。

【0030】管理者PIN(暗証番号)は管理している利用者の暗証番号を示し、管理者端末鍵は端末の操作を許容する情報を示し、前述の管理者PINとこの管理者端末鍵とが特定の関係を示さないときパーソナルファイルの読取り／書込みが許容されない。

【0031】前述のパーソナルファイルは、個人情報鍵とバイオ鍵との2つの小ファイルからなり、個人情報鍵は、照合時に鍵となる情報であり、適性が判定されないときは、次ぎの個人情報の読取り／書込みが許容されない。また、個人情報として、ユーザまたはオペレータを示す種別、氏名、IDコード、年齢、生年月日、住所、電話番号、会社名等を記録する。バイオ鍵は、照合時に鍵となる情報であり、適性が判定されないときは、次ぎのバイオメトリック情報に関する情報の読取り／書込みが許容されない。また、バイオメトリック情報として、指紋の特徴を示す情報、その指紋の属性データとして、照合レベル、照合スコアを記録する。なお、上述のバイオメトリック情報としては、指紋の他、声紋、網膜紋、顔面特徴、掌の紋など、個人を特定できる特徴部分が含まれる。

【0032】また、図4には開示していな情報として、各種のアプリケーションにセキュリティレベルを、例えば、レベル1，2，3のように複数段に設定し、これに対応して照合スコアを90%以上の照合、80%～90%の照合、70%～80%の照合のように設定すると、アプリケーションのセキュリイティに対応させて認証を得ることができる。

【0033】次ぎに、前述の認証装置10の処理動作を説明する。認証装置10を認証カード11を発行する機能を有し、該認証カード11の発行は係員によって行われ、この発行時には認証装置10にパーソナルコンピュータ(PC)が接続され、該PCから必要なカードデータが設定入力される。

【0034】上述の認証カード11を発行するための認証装置10のCPU20の処理を図5のフローチャートを参照して説明する。係員(オペレータ)には予めオペレータ用認証カード11と登録用のパスワードとが与えられており、表示器13にはパスワードの入力が案内表示され、係員が表示器13のタッチパネル23よりパスワードを入力すると、予めRAM22に記憶されていたパスワードと比較して、不一致の時は再度入力が要求され、一致したときは次ぎのステップに移行される(ステップn1，n2)。

【0035】次ぎのステップでは、表示器13にオペレータの認証カード11の挿入が案内表示され、この表示に基づいてオペレータの認証カード11が挿入口12に挿入されると、そのICコンタクト33がICカードリーダ24と接続して、該ICカードリーダ24でカードデータが読取られて、カードデータがチェックされ、すなわち、発行者鍵、管理者PIN、管理者端末鍵、個人情報鍵、バイオ鍵等がチェックされ、適性が認められると、表示器13にはオペレータのバイオメトリック情報の読取りが案内表示され、係員がバイオメトリックセンサ14に所定の指を載せて指紋を読取らせると、指紋情報が取込まれると共に、カードデータに設定されているバイオメトリック情報がその属性データの照合レベルおよび照合スコアに基づいて、照合し判定される(ステップn3，n4)。

【0036】上述の指紋情報の照合判定で一致または所定値の特徴量(照合スコア)の一致が判定されると、オペレータが認証されるので、該オペレータによる利用者の認証カード11の発行が許容される(ステップn5)。

【0037】係員によるユーザ用の認証カード11の発行が許容されると、係員は該認証装置10に接続されているパーソナルコンピュータ(PC)によりカードデータを作成するために、図4で示した各ファイルの必要事項をそのキーボード(入力手段)より入力し、次いで、挿入口12にユーザ用の認証カード11(ICカード)を挿入する(ステップn6，n7)。

【0038】次いで表示器13にはユーザ(利用者)のバイオメトリック情報の読取りが案内表示され、ユーザがバイオメトリックセンサ14に所定の指を載せて指紋を読取らせると、指紋情報が取込まれると共に、設定した属性データの照合レベルおよび照合スコアに基づいて、指紋の特徴量を読取る(ステップn8)。

【0039】このようにしてユーザの指紋情報がその属性データと共に確定すると、先に入力されている必要事項と共にしてカードデータが完成し、このカードデータがICカードリーダ24により認証カード11に書込まれてユーザ用認証カード11が完成する(ステップn9)。

【0040】その後、次ぎのユーザの認証カード11の発行があるか否かを判定し、次ぎの発行があるときはステップn6にリターンし、無いときは発行処理を終了する(ステップn10)。

【0041】次ぎに、認証装置10で既に発行したユーザ用認証カード11のカードデータを変更する場合の認証装置10のCPU20の処理を図6のフローチャートを参照して説明する。係員(オペレータ)には予めオペレータ用認証カード11と変更用のパスワードとが与えられており、表示器13

にはパスワードの入力が案内表示され、係員が表示器13のタッチパネル23よりパスワードを入力すると、予めRAM22に記憶されていたパスワードと比較して、不一致の時は再度入力が要求され、一致したときは次ぎのステップに移行される(ステップn11, n12)。
【0042】次ぎのステップでは、表示器13にオペレータの認証カード11の挿入が案内表示され、この表示に基づいてオペレータの認証カード11が挿入口12に挿入されると、ICカードリーダ24でカードデータが読取られて、カードデータがチェックされる。
【0043】すなわち、発行者鍵、管理者PIN、管理者端末鍵、個人情報鍵、バイオ鍵等がチェックされ、適性が認められると、表示器13にはオペレータのバイオメトリック情報の読取りが案内表示され、係員がバイオメトリックセンサ14に所定の指を載せて指紋を読取らせると、指紋情報が取込まれると共に、カードデータに設定されているバイオメトリック情報がその属性データの照合レベルおよび照合スコアに基づいて、照合し判定される(ステップn13, n14)。
【0044】上述の指紋情報の照合判定で一致または所定値の特徴量(照合スコア)の一致が判定されると、オペレータが認証されるので、該オペレータによるユーザ用認証カード11のカードデータ変更の操作が許容される(ステップn15)。
【0045】係員によるユーザ用の認証カード11の変更操作が許容されると、次いで、挿入口12にユーザ用の認証カード11(ICカード)を挿入する(ステップn16)。挿入された認証カード11はICカートリーダ24により読取られて、パーソナルコンピュータ(PC)の表示器に表示され、該パーソナルコンピュータ(PC)のキーボード(入力手段)よりカード所有者の変更があった個人情報をオペレータが修正し変更する。例えば、カード所有者の年齢の変更、住所の変更、電話番号の変更会社名の変更、その他の変更であって、変更のあった事項を修正する(ステップn17)次いで、カード所有者の指紋も変更されるのか否かを判定し(ステップn18)、変更がある場合は、表示器13にユーザ(利用者)のバイオメトリック情報の読取りが案内表示され、ユーザがバイオメトリックセンサ14に変更する指を載せて指紋を読取らせると、指紋情報が取込まれると共に、設定した属性データの照合レベルおよび照合スコアに基づいて、指紋の特徴量を読取る(ステップn19)。
【0046】このようにしてユーザの指紋情報がその属性データと共に確定すると、先に変更事項が入力されている必要事項と共にしてカードデータが完成し、このカードデータがICカードリーダ24により認証カード11に書込まれてユーザ用認証カード11の変更処理が完了する(ステップn20)。
【0047】その後、次ぎのユーザ用認証カード11の変更操作があるか否かを判定し、次ぎの変更操作があるときはステップn16にリターンし、無いときは処理を終了する(ステップn21)。
【0048】次ぎに、認証装置10のCPU20によるユーザ用認証カード11の本人認証の照合処理を図7のフローチャートを参照して説明する。係員(オペレータ)には予めオペレータ用認証カード11と照合用のパスワードとが与えられており、表示器13にはパスワードの入力が案内表示され、係員が表示器13のタッチパネル23よりパスワードを入力すると、予めRAM22に記憶されていたパスワードと比較して、不一致の時は再度入力が要求され、一致したときは次ぎのステップに移行される(ステップn31, n32)。
【0049】次ぎのステップでは、表示器13にオペレータの認証カード11の挿入が案内表示され、この表示に基づいてオペレータの認証カード11が挿入口12に挿入されると、ICカードリーダ24でカードデータが読取られて、カードデータがチェックされる。
【0050】すなわち、発行者鍵、管理者PIN、管理者端末鍵、個人情報鍵、バイオ鍵等がチェックされ、適性が認められると、表示器13にはオペレータのバイオメトリック情報の読取りが案内表示され、係員がバイオメトリックセンサ14に所定の指を載せて指紋を読取らせると、指紋情報が取込まれると共に、カードデータに設定されているバイオメトリック情報がその属性データの照合レベルおよび照合スコアに基づいて、照合し判定される(ステップn33, n34)。
【0051】上述の指紋情報の照合判定で一致または所定値の特徴量(照合スコア)の一致が判定されると、オペレータが認証されるので、該オペレータによるユーザ用認証カード11の本人認証の照合操作が許容される(ステップn35)。
【0052】係員によるユーザ用の認証カード11の変更操作が許容されると、次いで、挿入口12にユーザ用の認証カード11を挿入する(ステップn36)。挿入された認証カード11はICカートリーダ24により読取られて、パーソナルコンピュータ(PC)の表示器に表示され、次いで表示器13にはユーザ(利用者)のバイオメトリック情報の読取りが案内表示され、ユーザがバイオメトリックセンサ14に所定の指を載せて指紋を読取らせると、指紋情報が取込まれると共に、設定した属性データの照合レベルおよび照合スコアに基づいて、指紋の特徴量を読取る(ステップn37)。
【0053】次ぎに、認証カード11に記録されていたバイオメトリック情報と、センサ14で読取った利

用者の指紋によるバイオメトリック情報とを照合レベルおよび照合スコアに基づいて照合判定し（ステップn38）、一致したときは本人認証が得られたことになり、接点出力端子25（図2参照）から認証出力を出力する（ステップn39）。この出力により、これに接続された端末、例えば自動取引き処理装置等は能動化される。

【0054】なお、前述のステップn38で、一致が判定されないNGの時は、ステップn36にリターンして、再度照合操作を繰り返すことになるが、このNGが所定回数例えば3回になると、不正使用と判定して、認証カード11のヒューズROM34（図3参照）が破壊されて、認証カード11の使用が不可能になる。

【0055】また、上述のような認証照合の処理が連続してあるときは前述のステップn36にリターンされるが、無いときは処理を終了する（ステップn40）。

【0056】次ぎに、認証装置10を立ち上げるために必要なデータの設定処理をするCPU20の処理動作を図8のフローチャートを参照して説明する。係員（オペレータ）には予めオペレータ用認証カード11と設定用のパスワードとが与えられており、表示器13にはパスワードの入力が案内表示され、係員が表示器13のタッチパネル23よりパスワードを入力すると、予めRAM22に記憶されていたパスワードと比較して、不一致の時は再度入力が要求され、一致したときは次ぎのステップに移行される（ステップn41，n42）。

【0057】次ぎのステップでは、表示器13にオペレータの認証カード11の挿入が案内表示され、この表示に基づいてオペレータの認証カード11が挿入口12に挿入されると、ICカードリーダ24でカードデータが読取られて、カードデータがチェックされる。

【0058】すなわち、発行者鍵、管理者PIN、管理者端末鍵、個人情報鍵、バイオ鍵等がチェックされ、適性が認められると、表示器13にはオペレータのバイオメトリック情報の読取りが案内表示され、係員がバイオメトリックセンサ14に所定の指を載せて指紋を読取らせると、指紋情報が取込まれると共に、カードデータに設定されているバイオメトリック情報がその属性データの照合レベルおよび照合スコアに基づいて、照合し判定される（ステップn43，n44）。

【0059】上述の指紋情報の照合判定で一致または所定値の特徴量（照合スコア）の一致が判定されると、オペレータが認証されるので、該オペレータによる設定操作が許容される（ステップn45）。

【0060】係員による設定操作が許容されると、次いで、パーソナルコンピュータ（PC）の表示器に設定画面が表示され、設定データがキーボードにより入力される（ステップn46，47）。この設定データは、例えば、登録用、変更用、照合用、設定用の各パスワード、日付、適用カード、自動変更フラグ、変更処理フラグ、その他必要なデータである。

【0061】上述の設定データの入力および編集が終了すると、設定データが上位の機器にアップデートされ、設定処理を終了する（ステップn48，49，50）。

【0062】上述の実施例で示した認証カード11によれば、指紋によるバイオメトリック情報を、読み出し可能なICカードに記録して読み出し可能に構成したので、パーソナルコンピュータ（PC）のアプリケーション側には、操作の対象となる利用者全員のバイオメトリック情報を記憶手段に記憶して保存する必要がなく、アプリケーション側の記憶容量が極めて少なくて済む。また、1つの認証カード11を、例えば、銀行、クレジット社、郵便局、その他の金融機関、その他認証が必要な機関といつた業種の異なる複数のアプリケーションに対して使用することができ、便利性を有する。

【0063】また、バイオメトリック情報の属性情報として、例えば、バイオメトリック情報を読取るセンサ14の閾値レベルを設定した照合レベルや、バイオメトリック情報を照合して判定するときの基準値となる特徴点のポイント数を設定した照合スコアを記録すると、バイオメトリック情報を照合するためのセンサ14に読取り精度のバラツキがあっても、また、利用者側に読取り時の状態に多少変動があっても、照合精度を調整することにより、照合に必要な情報の読取りができ、また、認証装置が複数あっても、同じ条件で照合ができ、利用者が本人であっても機械側の問題で、認証不可となることが防止される。

【0064】さらに、バイオメトリック情報の属性情報として、複数のセキュリティレベルに対応した情報を記録しておくことにより、アプリケーション側のセキュリティレベルに対応した照合ができる。

【0065】さらに、認証処理を実行しても認証が得られない場合、第3者の不正利用と判定されるので、この場合、記録情報をヒューズROM34（破壊手段）で読取り不可能にすることにより、認証カード11のセキュリティを高めることができ、偽造防止対策にもなる。

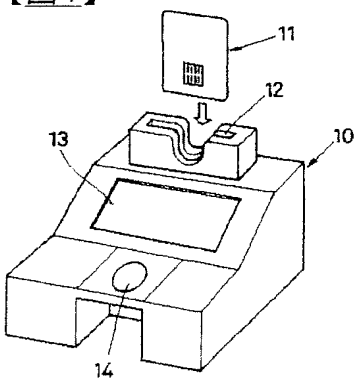
【0066】さらに、認証装置10にあっては、上述のような効果を奏する認証カード11の発行、および認証処理ができ、また、1台で認証媒体発行装置及び認証装置を兼ねることができる。

【0067】なお、上述の実施例ではバイオメトリック情報として指紋を示しているが、指紋の他、声

紋、網膜紋、顔面特徴、掌の紋など、個人を特定できる特徴部分で構成することができる。
【0068】この発明の構成と、上述の実施例との対応において、この発明の認証媒体は、実施例のICカードによる認証カード11、またはSIMチップに対応し、以下同様に、破壊手段は、ヒューズROM34，ヒューズROM書込み制御回路35、その他、物理的に認証カード11を破壊する手段に対応し、認証媒体発行装置の記録手段は、ICカードリーダ24に対応し、読取り手段は、バイオメトリックセンサ14に対応し、制御手段は、CPU20に対応し、入力手段は、パーソナルコンピュータ(PC)のキーボードに対応し、認証装置の第1の読取り手段は、ICカードリーダ24に対応し、第2の読取り手段は、バイオメトリックセンサ14に対応し、判定手段は、CPU20に対応するも、この発明は、特許請求の範囲に記載の技術的思想に基づいて応用することができ、実施例の構成のみに限定されるものではない。

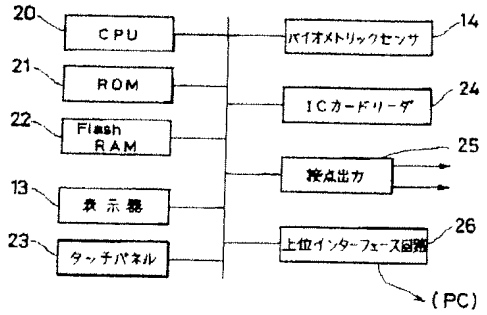
【図面の簡単な説明】
【図1】認証装置と認証カードの斜視図。
【図2】認証装置の制御回路ブロック図。
【図3】認証カードの制御回路ブロック図。
【図4】認証カードのカードデータの説明図。
【図5】認証カード登録処理のフローチャート。
【図6】認証カード変更処理のフローチャート。
【図7】認証カード認証照合処理のフローチャート。
【図8】認証カード設定処理のフローチャート。
【符号の説明】
10…認証装置
11…認証カード
14…バイオメトリックセンサ
20…認証装置のCPU
24…ICカードリーダ
34…ヒューズROM
35…ヒューズROM書込み制御回路

【図1】

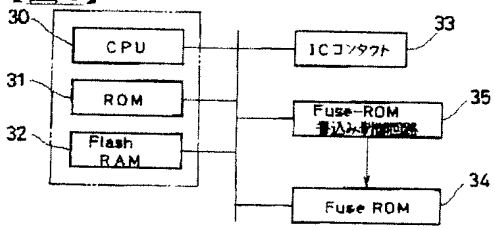


10 … 認証装置
11 … 認証カード
14 … バイオメトリックセンサ

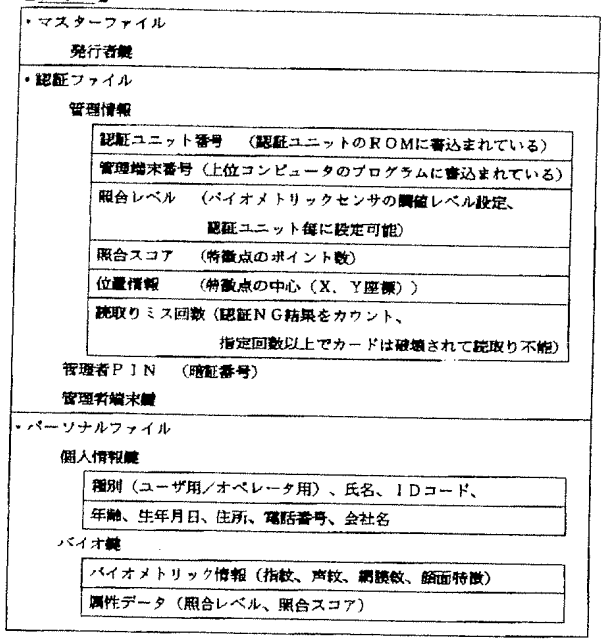
【図2】


20
CPU
21
ROM
22
Flash RAM
13
表示器
23
タッチパネル
バイオメトリックセンサ
14
ICカードリーダ
24
接点出力
25
上位インターフェース回路
26
(PC)

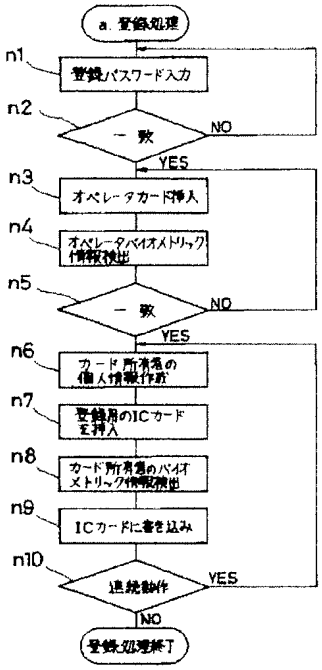
【図3】


30
CPU
31
ROM
32
Flash RAM
ICコンタクト
33
Fuse-ROM 書込み制御回路
35
Fuse ROM
34

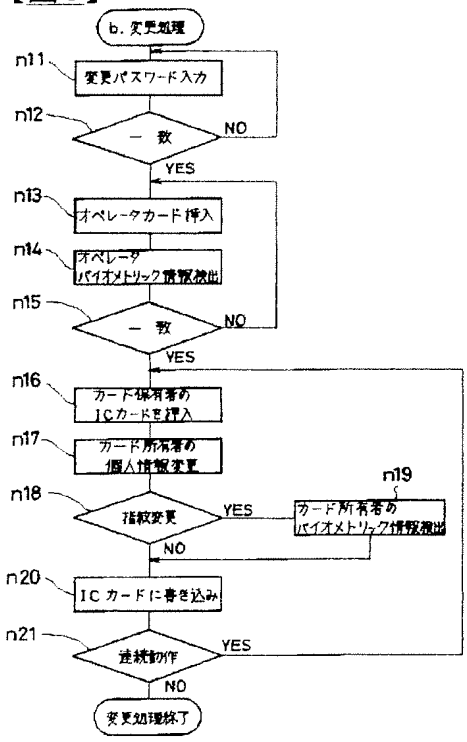
【図4】


・マスターファイル
発行者鍵
・認証ファイル
管理情報
認証ユニット番号 (認証ユニットのROMに書込まれている)
管理端末番号 (上位コンピュータのプログラムに書込まれている)
照合レベル (バイオメトリックセンサの閾値レベル設定、認証ユニット毎に設定可能)
照合スコア (特徴点のポイント数)
位置情報 (特徴点の中心 (X、Y座標))
読取りミス回数 (認証NG結果をカウント、指定回数以上でカードは破壊されて読取り不能)
管理者PIN (暗証番号)
管理者端末鍵
・パーソナルファイル
個人情報鍵
種別 (ユーザ用/オペレータ用)、氏名、IDコード、
年齢、生年月日、住所、電話番号、会社名
バイオ鍵
バイオメトリック情報 (指紋、声紋、網膜紋、顔面特徴)
属性データ (照合レベル、照合スコア)

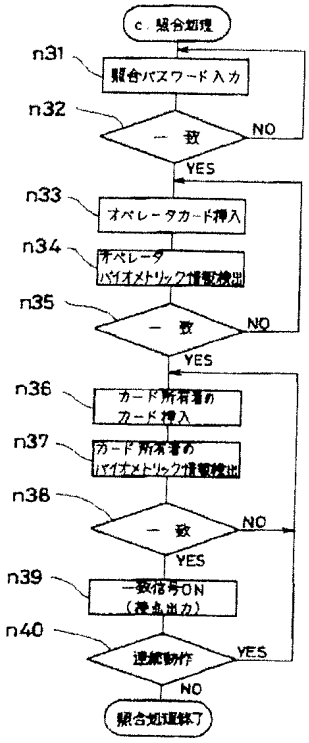
【図5】


a. 登録処理
n1
登録パスワード入力
n2
一 致
NO
YES
n3
オペレータカード挿入
n4
オペレータバイオメトリック情報検出
n5
一 致
NO
YES
n6
カード所有者の個人情報作成
n7
登録用のICカードを挿入
n8
カード所有者のバイオメトリック情報検出
n9
ICカードに書き込み
n10
連続動作
YES
NO
登録処理終了

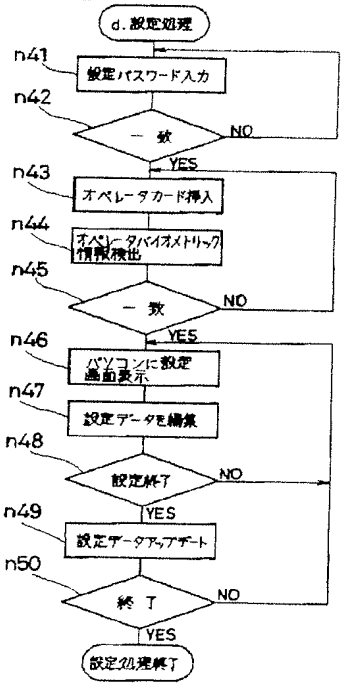
【図6】


b. 変更処理
n11
変更パスワード入力
n12
一 致
NO
YES
n13
オペレータカード挿入
n14
オペレータバイオメトリック情報検出
n15
一 致
NO
YES
n16
カード保有者のICカードを挿入
n17
カード所有者の個人情報変更
n19
n18
指紋変更
YES
カード所有者のバイオメトリック情報検出
NO
n20
IC カードに書き込み
n21
連続動作
YES
NO
変更処理終了

【図7】


c. 照合処理
n31
照合パスワード入力
n32
一 致
NO
YES
n33
オペレータカード挿入
n34
オペレータ
バイオメトリック情報検出
n35
一 致
NO
YES
n36
カード所有者の
カード挿入
n37
カード所有者の
バイオメトリック情報検出
n38
一 致
NO
YES
n39
一致信号ON
（接点出力）
n40
連続動作
YES
NO
照合処理終了

【図8】


d. 設定処理
n41
設定パスワード入力
n42
一 致
NO
YES
n43
オペレータカード挿入
n44
オペレータバイオメトリック
情報検出
n45
一 致
NO
YES
n46
パソコンに設定
画面表示
n47
設定データを編集
n48
設定終了
NO
YES
n49
設定データアップデート
n50
終 了
NO
YES
設定処理終了